

PARADIGMA ZAŠTITE DISTRIBUIRANOG RAČUNARSTVA

Gojko Grubor¹

Angelina Njeguš²

Nenad Ristić³

Univerzitet Singidunum

Danijelova 32, Beograd

Tel: +381 11 3093-236

¹e-mail: ggrubor@singidunum.ac.rs

²e-mail: anjegus@singidunum.ac.rs

³e-mail: nristic@sinergija.edu.ba

Sažetak: Nove sofisticirane pretnje za veb 2.0 i veb 3.0 aplikacije zahtevaju novu paradigmu zaštite informacija. Novi tipovi crva (Yamanner, Samy i Spaceflash) već su (2009) iskoristili ranjivost AJAX okvira na klijentskoj strani, obezbedili novi tip napada i kompromitovali neke poverljive informacije. Trend razvoja računarstva je virtuelizacija servera i klijenta, više podataka u saobraćaju, primena socijalnih mreža u poslovnim sistemima, unificirane komunikacije, jeftine ili besplatne mobilne i bežične aplikacije i distribuirano računarstvo (cloud computing). Tekući trend razvoja računarstva zahteva novu paradigmu zaštite, jer tradicionalne kontrole zaštite nisu dovoljne, a često ni adekvatne. U radu su predstavljena dva nova modela zaštite distribuiranog računarstva.

Ključne reči: ranjivost veb aplikacija, virtuelizacija, distribuirano računarstvo, ugrađena zaštita, model digitalnih mrava

Abstract: New sophisticated treats to web 2.0 i web 3.0 applications need a new security information paradigm. Some new type of worms (Yamanner, Samy and Spaceflash) have already exploited AJAX client frame vulnerability and provided new types of attacks and compromised certain confidential information. Computing development trend includes server and client virtualization, more data trafic, use of social networks in organizations, unified communications, chip or free mobile and wireless applications and cloud computing. Curent comuting development trend requests a new security information paradigm. Traditional security controls do not suficient and often inadequate. The two new cloud computing security models are presented in this piece of paper.

Key words: web applications vulnerability, virtualization, cloud computing, enbeded security, digital ants' model

1. UVOD

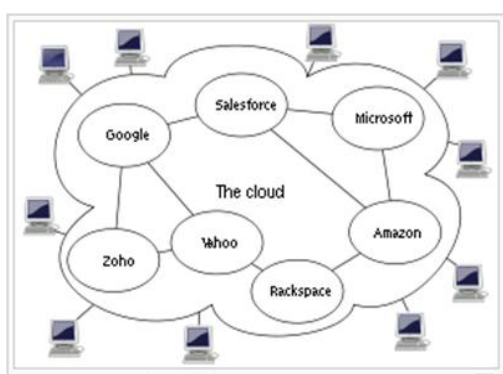
Novi tipovi pretnji i bezbednosni aspekti veb 2.0 i veb 3.0 aplikacija, zahtevaju novu paradigmu zaštite informacione imovine poslovnih sistema. Tehnološke transformacije i evolucija veba u veb 2.0 i veb 3.0, otvaraju nove bezbednosne izazove i nove vektore napada na veb aplikacije. Novi tipovi crva (Yamanner, Samy i Spaceflash) već su iskoristili ranjivost AJAX (Asynchronous JavaScript + XML) okvira na klijentskoj strani, obezbedili novi tip napada i kompromitovali neke poverljive informacije.

Trendovi razvoja računarstva u sledećih 5 godina su virtuelizacija servera i klijenta, više podataka u saobraćaju (rast za 650%), primena socijalnih mreža u poslovnim sistemima, unificirane komunikacije, jeftine ili besplatne mobilne i bežične aplikacije i distribuirano računarstvo (*cloud computing*). Tekući trendovi razvoja računarstva, takođe, zahtevaju novu paradigmu zaštite, jer tradicionalne kontrole zaštite nisu dovoljne, a često ni adekvatne [7].

2. PARADIGMA ZAŠTITE DISTRIBUIRANOG RAČUNARSTVA

2.1. Funkcionalni aspekti distribuiranog računarstva

Koncept distribuiranog računarstva (DR) uključuje razvoj i upotrebu IT i računarstva zasnovanog na Internetu (Sl. 1), gde korisnici apstrahuju detalje i nemaju potrebu da poznaju ili kontrolišu tehnološku infrastrukturu u „oblaku“ (metafori Interneta), koja ih podržava obezbeđivanjem servisa preko Interneta: dinamičkih, skalabilnih i virtuelizovanih resursa (hardverskih, softverskih, platformi, za skladištenje itd.) [1][2].



(a)



(b)

Slika 1. Logički dijagram (a) i metafora distribuiranog računarstva (b) [1]

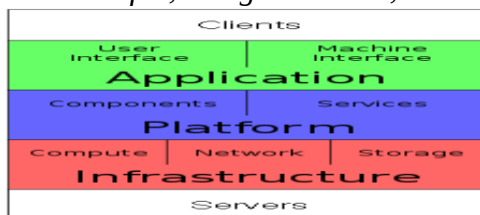
Tipično servise DR obezbeđuju uobičajene *online* poslovne aplikacije, kojima korisnici pristupaju sa veb pretraživačem, dok su programi i podaci uskladišteni na veb serverima. Ovi servisi se generalno dele u tri kategorije: (1) *Infrastruktura kao servis (IaaS)*, (2) *Platforma kao servis (PaaS)* i (3) *Softver kao servis (SaaS)*.

Ključne karakteristike DR su: *agilnost, manji troškovi, nezavisnost tipa uređaja i lokacija, istovremeno deljenje i iznajmljivanje resursa* brojnim korisnicima, *pouzdanost* (redundantnost resursa), *skalabilnost resursa* prema dinamici zahteva, *održivost i bezbednost*, koja je generalno jednaka ili veća od bezbednosti tradicionalnih sistema, zbog centralizacije resursa, ali ranjivija zbog lakšeg gubitka kontrole nad osetljivim podacima i nedovoljne zaštite distribuiranih jezgara (kernela) OS u dinamički promenljivom virtuelnom okruženju.

Funkcionalne slojeve sistema DR (Sl. 2) čine distribuirani: *klijenti, aplikacije, platforme, infrastruktura i serveri*.

Distribuirani klijenti (*Cloud clients*) se sastoje od računarskog hardvera i/ili softvera koji se oslanja na DR za isporuku aplikacija, ili su specifično dizajnirani za isporuku *distribuiranih* servisa bez kojih su, u suštini, nekorisni. Primeri su: mobilni uređaji (*Android, iPhone*,

Windows Mobile), tanki klijenti (*CherryPal*, *Zonbu*, g_OS-bazirani sistemi) i debeli klijenti/veb pretraživači (*Mozilla Firefox*, *Google Chrome*, *WebKit* i dr.).



Slika 2. Funkcionalni slojevi DR [1]

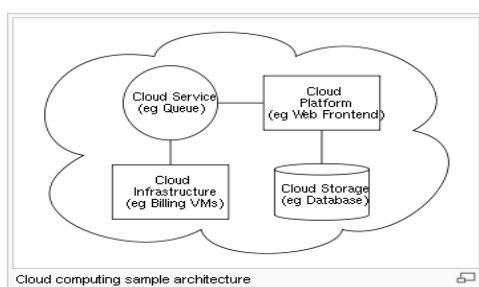
Distibuirane aplikacije (*Cloud aplikations*) eliminišu potrebu za instaliranjem i upotrebom aplikacije na korisničkom računaru. Primeri su: peer-to-peer (*BOINC*, *Skype*), veb aplikacije (*Facebook*, *Twitter*, *YouTube*), servisi zaštite (*MessageLabs*, *Purewire*, *ScanSafe*, *Zscaler*), servisi softvera (*A2Zapps.com*, *Google Apps*, *Salesforce*) i ekstra softverski servisi (*Microsoft Online Services*).

Distibuirana platforma (PaaS) isporučuje računarske platforme kao servis, a generalno koristi *distibuiranu* mrežnu infrastrukturu i podržava *distibuirane* aplikacije, kao što su:

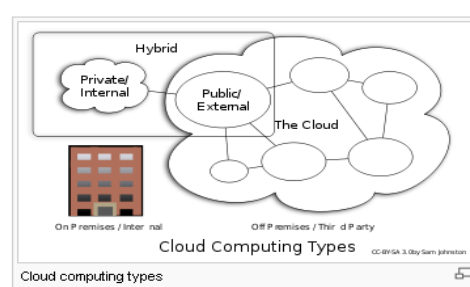
- Servisi: identifikacije (*OAuth*, *OpenID*), plaćanja (*Amazon Flexible Payments Service*, *Google Checkout*, *PayPal*), pretrage (*Alexa*, *Google Custom Search*, *Yahoo! BOSS*) i realnog-sveta (*Amazon Mechanical Turk*)
- Stekovi za rešenja (*Solution stacks*): Java (*Google App Engine*), PHP (*Rackspace Cloud Sites*), Python Django (*Google App Engine*), Ruby on Rails (*Heroku*), .NET (*Azure Services Platform*, *Rackspace Cloud Sites*) itd.
- Struktuirana skladišta podataka: baze podataka (*Amazon SimpleDB*, *BigTable*), skladištenje fajlova (*Amazon S3*, *Nirvanix*, *Rackspace Cloud Files*, *Diomedee Storage*)

Infrastruktura DR-a sastoji se uglavnom od servisa isporučivanih kroz centre za obradu podataka i generisanih na serverima sa različitim stepenom virtuelizacije (2009). Osnovu za većinu implementacija čine softveri sa otvorenim kodom, najčešće sa jednom pristupnom tačkom za sve klijente. Korisnici DR-a ne poseduju sopstvenu fizičku infrastrukturu, a resurse iznajmljuju kao servis poverljivog provajdera usluga i plaćaju samo ono što koriste (kao potrošnju struje ili vode), ili na bazi pretplate. Aranžmani su pokriveni sa ugovorom o nivou usluga - SLA (*Service Level Agreement*), kojeg korisnici mogu uvek prekinuti.

Serverski sloj sadrži računarski hardver i softver specifično dizajnirane za isporuku distribuiranih servisa, kao na primer *Fabric computing* (*Cisco UCS*). Tipičan primer **arhitekture DR-a** prikazan je na slici 3a, a tipovi DR-a na slici 3b.



(a)



(b)

Slika 3. Primer arhitekture DR (a) i tipova DR (b) [1]

Generalno, infrastruktura, arhitektura i tipovi DR (Tabela 1) zahtevaju značajnu izmenu paradigme klasičnog sistema zaštite IS organizacija.

Tabela 1. Tipovi DR

Tip DR	Opis
Javno	dinamički obezbeđuje servise, na bazi samousluge preko Interneta putem veb aplikacija/veb servisa provajdera usluga koji deli resurse i naplaćuje usluge
Hibridno	veći broj internih i eksternih provajdera, tipično za većinu organizacija
Privatno	vendori ga koriste da opišu svoje ponude emulacije DR na privatne računarske mreže

2.2. Nova paradigma zaštite veb aplikacija distribuiranog računarstva

Pristup tehnologijama DR (*SaaS, PaaS, IaaS*) zahteva tankog klijenta, što je obično veb pretraživač. Danas se veći deo novca za zaštitu troši na barijere (*firewalls*) i antivirusne programe (AVP). Poslednjih 10 godina vektori napadi se pomeraju sa mrežnog na aplikativni OSI sloj, zato što su OS i servisi dostupni sa Interneta izolovani sa DMZ. Lakše je napasti logiku ili okvir neke aplikacije, nego aktuelni server zaštićen sa DMZ. Aplikacije većinom razvijaju organizacije za svoje potrebe, pri čemu neke ne smatraju da je bezbednost najviši prioritet, što dovodi do brojnih i različitih ranjivosti sistema zaštite. DR nije dizajnirano sa aspekta bezbednosti, iako organizacije kao što su CSA (*Cloud Security Alliance*) i OWASP (*Open Web Application Security Project*) čine napore da reše brojne bezbednosne probleme DR (npr., CSA je definisala *distribuiranu barijeru* za veb aplikacije).

2.2.1. Tehnologije zaštite veb aplikacija

Za razliku od AVP programa koji radi na bazi potpisa (definicije) i po principu: *dopusti sve osim poznatih malicioznih programa*, desktop barijere su efektivna odbrana od napada nultog-dana, promene zapisa malicioznih kodova i mrežnih napada, jer slede prosto pravilo: *ne dozvoliti nikakav saobraćaj u mrežu, dok to korisnik ne dopusti*. Slabost barijera je što generalno dopuštaju korisnički iniciran HTTP saobraćaj na TCP portu 80. Većina istraživanja pokazuje da *spyware* i drugi maliciozni programi postoje na preko 80% PC računara koji imaju barijere, [4]. Barijere ne mogu sprečiti ni direktan prolaz malicioznog programa. Desktop barijere, kritične za zaštitu računara u krajnjoj tački, nisu potpuno efektivne za zaštitu veb aplikacija, jer ih savremeni napadi uspešno zaobilaze. Zato je potrebna dodatna zaštita na krajnjoj tački, posebno za veb pretraživač, koji treba da ima štit za apsorpciju napada i zaštitu identiteta i podataka. Tehnologije za zaštitu veb aplikacija mogu se klasifikovati u dve osnovne kategorije: *manuelno virtuelizovan sistem i sistem blokiranja metoda napada* [6].

Manuelno virtuelizovan sistem koristi metod *precizne emulacije* (*precision emulation*), virtuelizuje sav ili deo host računara i zahteva da se sve promene sa Interneta na PC događaju samo u virtuelnom okruženju. Za zaustavljanje veb-baziranih napada, prvi korak je izbor pravih komponenti OS i relevantnih aplikacija za virtuelizaciju. Cilj virtuelizacije je zaštita veb sesije korisnika, zatvaranjem u „zaštitni balon“ u toku pretraživanja, uz zadržavanje procesa jednostavnim i transparentnim za korisnika. Proces se nazva *preciznom emulacijom* zato što se virtuelizuju samo oni delovi OS kojima veb pretraživač može pristupiti i nema

potrebe da korisnik prati trag u brojnim OS ili fajl sistemima. Program za virtuelizaciju automatski održava virtuelni sistem kojeg kreira.

Svaki put kad korisnik pretražuje veb, brojne promene se dešavaju na njegovom računaru (većina je bezopasnih). Specifičan slučaj je procesiranje *online* formulara za registrovanje na veb lokaciju, kada server te lokacije često kreira kolačić (*cookie*) koji pretraživač smešta na računar korisnika. U procesu precizne emulacije, program za virtuelizaciju sledi jednostavno pravilo barijera. Korisnički inicirana preuzimanja (*downloads*) sa Interneta upisuju se na računar na uobičajen način, dok se sva druga preuzimanja upisuju na *emulacioni sloj*, koji nikada ne dodiruje računar. Tako pretraživač može posetiti svaku veb stranicu, zato što će se sve nepoznate/neželjene promene dogoditi na virtuelizovanom fajl sistemu, a ne krajnjem PC.

Metod *precizne emulacije* presreće MS Windows interfejse za direktan pristup fajlovima i ključevima registra, kreirajući dve glavne komponente: (1) program (*engine*) za kreiranje duplikata Windows fajlova i registara sistema i (2) program (*engine*) za maskiranu emulaciju (*under hood*) koji selektivno preusmerava pozive NT kernelu za virtuelizaciju i odlučuje da li je poziv kernelu korisnički ili automatski iniciran. Na kraju svake sesije pretraživanja virtuelni sloj se može resetovati. Bez ovog pristupa, korisnički nalog često aktiviran sa administrativnim privilegijama, daje aplikacijama slobodu da čitaju i upisuju u OS i kernel, što omogućava malicioznim programima pristup OS. Postavljanje *virtuelnog štita* oko pretraživača ima tri ključne bezbednosne prednosti:

1. *Ne zavise od potpisa*: sistem nultog-dana koji koristi pravila slična barijeri – odbija sve promene na računaru korisnika, osim ako ih sam korisnik ne inicira.
2. *Štiti računar korisnika od trenutka priključivanja na Internet*: virtuelizovani zaštitni sloj štiti računar korisnika od trenutka logovanja na veb lokaciju pa do kraja sesije.
3. *Nije zahtevan*: ne traži posebno podešavanje ili održavanje od strane administratora, a sve aktivnosti virtuelizacije su nevidljive za korisnika.

Sistem blokiranja metoda napada uklanjanja metod koji haker koristi da izvrši napad ili jednu ili više poznatih ranjivosti, koje dopuštaju hakeru da ubaci maliciozni kôd. Na ovaj način blokira se najčešće samo jedna napad, što nije dovoljno za razne veb napade.

2.2.2. Distribuirana zaštitna barijera

Za poverljivog provajdera servisa DR, zaštita postaje veoma kompleksna. Prosečan provajder može imati preko 10.000 klijenata, pretplaćenih za servise i sa različitim politikama, čak i unutar jedne organizacije. Tako provajder servisa DR mora upravljati sa n-stepenim podešavanjem filtriranja barijere na aplikativnom nivou. Postojeće veb aplikacione barijere (WAF) i druga rešenja zaštite su uglavnom ograničena na hardverske uređaje, što je problem za provajdere servisa DR, koji treba da imaju pune rekovne namenskih WAF uređaja (jedan po klijentu). Od provajdera servisa DR zahteva se zaštita potpuno virtuelizovanog okruženja, [8].

Idealno bi bilo da su aplikacije dizajnirane tako da se kontrole zaštite integrišu (ugrade) direktno u aplikacije i rešavaju suštinski problem postojećeg DR. Zaštita veb aplikacija u DR treba da bude *skalabilna, fleksibilna, virtuelna i laka za upravljanje*. WAF mora izbeći hardverska ograničenja i biti sposoban da dinamički skenira CPU, računare, rekovne servera i granice centara za obradu podataka, prilagođenih zahtevima individualnih korisnika. Trošenje resursa ovih *distribuiranih WAF* (DWAF) mora biti minimalno i usmereno na

detekciju/sprečavanje napada. Savremeni provajderi servisa DR koriste različite tradicionalne i virtuelne tehnologije u radu, tako da se idealan DWAf mora prilagoditi ovom mešovitom okruženju i biti dostupan kao *virtuelna softverska aplikacija, plug-in, SaaS* ili da se može integrisati u postojeći hardver. Fleksibilnost znači da DWAf minimalno utiče na postojeće računarske mreže. Veb baziran korisnički interfejs mora omogućiti korisniku da lako administrira svoje aplikacije. Konfigurisanje DWAf treba da se zasniva na zaštićenoj aplikaciji, a ne definisano sa zahtevima jednog hosta i mora omogućiti konfigurisanje sa mnogo većom granulacijom za svaku aplikaciju. Svaki set pravila za konfigurisanje DWAf mora biti podržan sa čarobnjakom za podešavanje. Statistički podaci, logovanje i izveštavanje moraju biti intuitivni, laki za korišćenje i integrisani u druge sisteme. Takođe, mora biti na raspolaganju sistem sa više administratorskih privilegija za efektivno upravljanje vrlo različitim zahtevima politika zaštite, kao i set mehanizama za zaštitu jezgara distribuiranih sistema.

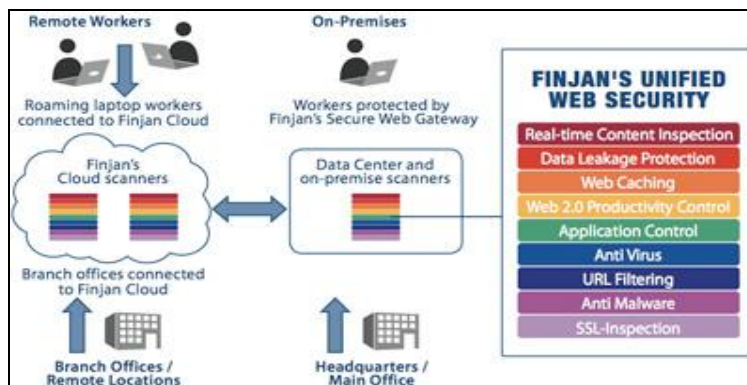
Sistemi za detekciju i sprečavanje upada (IDPS) u realnom DWAf sistemu, moraju izbegavati lažne pozitive i omogućiti skriveni monitoring, detekciju i potpunu transparentnost seta pravila za administratora. Poželjno je koristiti *skener veb ranjivosti*, inteligentne *algoritme* ili *statički analizador izvornog kôda* za sugerisanje seta pravila. Kako detekcija upada nije dovoljna za zaštitu veb aplikacija u DR, preporučuje se *proaktivna zaštita sa virtuelnim štitom*. Mehanizmi za transparentno upravljanje zaštićenom sesijom, šifrovanje URL i virtuelizaciju forme i polja na nivou DWAf, a ne same aplikacije, mogu biti jaki faktori odvratanja za svakog napadača. Poželjno je da DWAf ima i *autentifikacioni okvir*, kao dodatni sloj zaštite perimetra. Na kraju DWAf se mora lako integrisati u postojeće tehnologije zaštite da bi obezbedio najbolju praksu slojevitosti zaštite veb aplikacija u DR. Za zaštitu servisa u DR predloženo je 7 vodećih principa (Tabela 2) [5].

Tabela 2. Glavni principi zaštite DR

Princip zaštite DR	Opis
1.	Mehanizme zaštite ugraditi, a ne samo integrisati, u infrastrukturu IS
2.	Razviti ekosistem različitih rešenja, proizvoda i servisa zaštite od opštih bezbednosnih problema
3.	Kreirati beskontaktni i transparentni sistem zaštite
4.	Obezbediti centralizovano upravljanje i korelaciju kontrola zaštite u odnosu na sadržaj
5.	Zaštiti informacije u pokretu kroz informacionu infrastrukturu DR od napada spolja i iznutra
6.	Dinamičku zaštitu zasnivati na proceni rizika za infrastrukturu i informacije
7.	Uspostaviti samoobučavajući sistem zaštite za praćenje u realnom vremenu dinamičku prirodu IT infrastrukture DR i malicioznih napada

2.2.3. Studija slučaja 1: Integrisano hibridno rešenje zaštite DR i veb servisa

Rešenje za zaštitu veb servisa *Vital Cloud* i *Vital Cloud Hybrid*, prikazano je na slici 4 [2].



Sl. 4. Rešenje za zaštitu veb servisa [Vital Cloud](#) i [Vital Cloud Hybrid](#) [2]

Koristeći aktivnu tehnologiju za ispitivanje sadržaja u realnom vremenu, rešenje štite sve korisnike od veb 2.0 napada. Hibridno rešenje integriše *EC2 distribuiranu platformu* (Amazon) sa rešenjem zaštite veba na lokaciji organizacije (*Finjan*). Ključne karakteristike rešenja *Vital Cloud Enterprise Web security* su prikazane u Tabeli 3.

Tabela 3. Karakteristike *Vital Cloud Enterprise Web security* rešenja

Karakteristika	Opis
Centralno upravljanje	prilagodljivo svim korisnicima i lokacijama, sa sinhronizovanim aplikacijama u organizaciji i distribuiranim skenerima sa politikom zaštite
Višeslojna veb zaštita bez granica	ostvaruje se <i>Finjan Vital Cloud</i> ispitivanjem sadržaja u realnom vremenu i detekcijom pretnji u nultom danu
Trenutno skeniranje gore i dole	obezbeđuje maksimalnu fleksibilnost za prilagođavanje promenama poslovnih potreba, gde se distribuirani skeneri mogu dodati/ukloniti za desetak sekundi
Redukcija ukupnih troškova	kombinovanjem unificirane bezbedne veb mrežne kapije na lokaciji organizacije sa distribuiranim skenerima
Fleksibilna implementacija	<i>Finjan Vital Cloud Hybrid</i> rešenje obezbeđuje efektivan balans zaštite sistema na lokaciji organizacije i distribuiranih skenera za svakog klijenta
Redukcija ukupnih troškova	obezbeđuje da poverljivi podaci ostaju u granicama organizacije i ne skladište se u distribuiranom okruženju

Objavljen je i metod arhiviranja e-pošte sa šifrovanjem na bazi politike zaštite [9]. Šifrovanje na bazi politike zaštite obezbeđuje zaštitu poruka i priloga u toku prenosa s kraja na kraj, bez značajne intervencije pošiljaoca (manuelnog izbora poruka za šifrovanje). Metod automatizuje proces šifrovanja sa programom (*engine*) na bazi pravila, koji pokreće TLS (*Transport Layer Security*) protokol i omogućava administratoru da pre-definiše tipove poruka koje treba šifrovati pre slanja. Za dodatni sloj zaštite, sve poruke se skladište šifrovane sa 256-bitnim AES u distribuiranu bazu arhivskih podataka, koja se u celini nalazi na redundantnom *SAS-70 II, Tier-4* centru za obradu podataka. Da se eliminiše intervencija krajnjeg korisnika, šifrovanje na bazi politike zaštite automatski *taguje* svaki e-mail za šifrovanje, koji se zatim isporučuje u geografski distribuirane *LiveOffice* centre za obradu podataka kroz bezbedan SSL/TLS-šifrovan tunel. Zatim se svaka poruka skenira u skladu sa politikom korišćenja i filtriranja e-mail poruka, šifrjuje i isporuči u korisnikov *Inbox* ili centralno uskladišti u bezbedan repozitorijum za pristup preko veb portala. Portalu se pristupa standardnim SMTP protokolom, koji alarmira primaoca da je stigla šifrovana poruka. Kada

korisnik preko portala pristupi e-mail poruci, može je čitati, odgovoriti na nju i kreirati nove poruke, takođe zaštićene šifrom na bazi politike zaštite [10].

2.2.3. Studija slučaja 2: Model Inteligencije kolonije digitalnih mrava



U beskonačnoj borbi za zaštitu računarskih mreža od napada, eksperti za zaštitu rade na razvoju novog modela odbrane, simulirajući rad kolonije mrava. Za razliku od tradicionalnih, statičkih hardversko-softverskih uređaja za zaštitu, novi *inteligentni agenti za zaštitu* („digitalni mravi“) lutaju kroz računarsku mrežu tražeći agente pretnji (viruse, crve,...). Kada *digitalni mrav* otkrije pretnju, programiran je da brzo privuče roj drugih *digitalnih mrava* na tu lokaciju, kao i pažnju administratora zaštite da pokrene istragu kompjuterskog incidenta. U osnovi ovog modela je koncept tzv. „inteligencije kolonije“ (*swarm intelligence*), koja obećava potpunu transformaciju postojeće zaštite kibernetičkog prostora. Kao što se kolonija mrava lako prilagođava dinamičkim promenljivim pretnjama - veoma brzo se skupe da blokiraju pretnju (uljeza) i brzo vrte redovnim zadacima, naučnici pokušavaju da realizuju isti model u računarskom sistemu [3].

Postojeći *reaktivni* sistemi i uređaji zaštite su dizajnirani da neprekidno štite računarske sisteme i mreže od svih *poznatih* pretnji. Kako brojni maliciozni programi modifikuju svoj kôd u prva 24 časa posle implementacije na Internetu, antivirusni programi (AVP) ih često ne mogu detektovati i ukloniti. Troše se računarski resursi za dugotrajno skeniranje, računari rade sporije, što sve iritira korisnike računara. Rešenje je razvoj bržeg metoda skeniranja, na bazi tehnike *paralelnog procesiranja*, gde se računarski podaci dele u *batche* fajlove koji se procesiraju paralelno, slično istim vrstama roba poredanih u rafovima u supermarketu, a svaka linija rafova je podložna određenom tipu pretnji.

U prototipu *digitalnih mrava*, implementiran je koncept *inteligencije kolonije* u čijoj osnovi je deljenje procesa AVP skeniranja prema specifičnim pretnjama. Prototip je ispitan na računarskoj mreži od 64 računara. Cilj projekta je implementirati 3.000 različitih tipova digitalnih mrava, od kojih svaki traga za različitim dokazom pretnje. Dok se kreću kroz računarsku mrežu, *digitalni mravi* ostavljaju *digitalne tragove*, modelovane prema tragovima mirisa koje ostavljaju mravi da bi doveli druge mrave do mesta napada. Svaki put kada digitalni mrav identifikuje neki dokaz pretnje, programiran je tako da iza sebe ostavi jači *digitalni trag*, koji privlači veći broj *digitalnih mrava*. Takav roj digitalnih mrava označava potencijalnu infekciju računara. U pilot projektu ubačen je crv u mrežu i digitalni mravi su ga uspešno otkrili.

Novi model zaštite najviše odgovara za velike mreže koje dele resurse i imaju veliki broj identičnih mašina (državne organizacije, velike korporacije i univerziteti). Korisnici računara, mogu biti sigurni da roj digitalnih mrava neće greškom ostati u njihovim računarima, zato što digitalni mravi ne mogu preživeti bez specifične programske aplikacije („čuvara kolonije“) instalirane na svakoj mašini, koja izveštava „mrežne stražare“. Administrator sistema monitoriše i nadgleda *koloniju digitalnih mrava* i kontroliše sve procese.

3. ZAKLJUČAK

Novi tipovi pretnji za veb 2.0 i veb 3.0 aplikacije, zasnovane na virtuelizaciji klijentske i serverske strane, otvaraju nove vektore napada na veb aplikacije i zahtevaju novu paradigmu

zaštite informacione imovine poslovnih sistema. Organizacije često imaju pogrešnu predstavu da tradicionalne kontrole zaštite krajnjih tačaka poslovnog IS, pružaju adekvatnu zaštitu od veb zasnovanih pretnji. Metodi napada se menjaju, uključujući načine prenosa i infekcije malicioznim programima i postaju sve sofisticiraniji. Veb napade je sve teže zaustaviti, a posledice postaju sve ozbiljnije. Tradicionalna zaštita je još uvek važna, ali ne može potpuno zaustaviti nove veb napade, jer nije usmerena na prave objekte. Potrebne su nove kontrole zaštite. Zaštita veb servisa i aplikacija mora se proširiti na ponašanje korisnika, kao i na zaštitu računarskih programa i konfiguracija. Metodi zaštite na bazi potpisa (definicije) ne mogu sami zaustaviti nove tipove napada niti jednostavno ukloniti maliciozne programe. U radu su prikazane nove tehnologije i dva nova modela zaštite veb 2.0 i veb 3.0 aplikacija i servisa virtuelizovanog DR – *integrisano hibridno rešenje* i model *inteligencije kolonije digitalnih mrava*, kao i arhitektura DWARF (distribuirane veb barijere), virtuelnog štita veb aplikacija, tipova šifrovanja i autentifikacije koji mogu predstavljati ozbiljni faktor odvracanja napadača

4. LITERATURA

- [1] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, December 2009.
- [2] Finjan, *Vital Cloud and Vital Cloud Hybrid solution for cloud computing protection*, Seurity News 2009.
- [3] Fulp E., Wake Forest Univerzity, Fink G., Pacific Northwest National Laboratory (PNNL), Richland, Washinton, SAD; Featherstun W., i Williams B., Wake Forest Univerzity, *Project Digital Ants*, Seurity News 2009.
- [4] IBM, *IBM X-Force 2008 Annual Report*, www.ibm.org, 2008
- [5] *LiveOffice Reports*, Security News, oktobar 2009.
- [6] Lowe N., *Protecting browsers, endpoints and enterprises against new Web-based attacks*, InSecure, issue 23, page 33, novembar 2009
- [7] Mather T., Kumaraswamy S., Latif S., *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) (Paperback)*, O'Reilly, 2009
- [8] Meisel A., *Art of Defence*, Security News, 23.7. 2009.
- [9] RSA, *2009RSA Conference Europe*, Seurity News, septembar 2009.
- [10] Sun Microsystems, *Advanced cloud security tools*, CSA Seurity News, decembar 2009